NASA Procedural Requirements

NPR 8715.7
Effective Date: May 30, 2008
Expiration Date: May 30, 2013

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Expendable Launch Vehicle Payload Safety Program

Responsible Office: Office of Safety and Mission Assurance

Chapter 2. Safety Review and Approval Process

2.1 Introduction

This chapter identifies the roles, responsibilities, and requirements that are specific to the NASA ELV payload safety review and approval process, including the required sequence of activities and associated deliverables. For each NASA ELV payload project, the overall goals of this process are to:

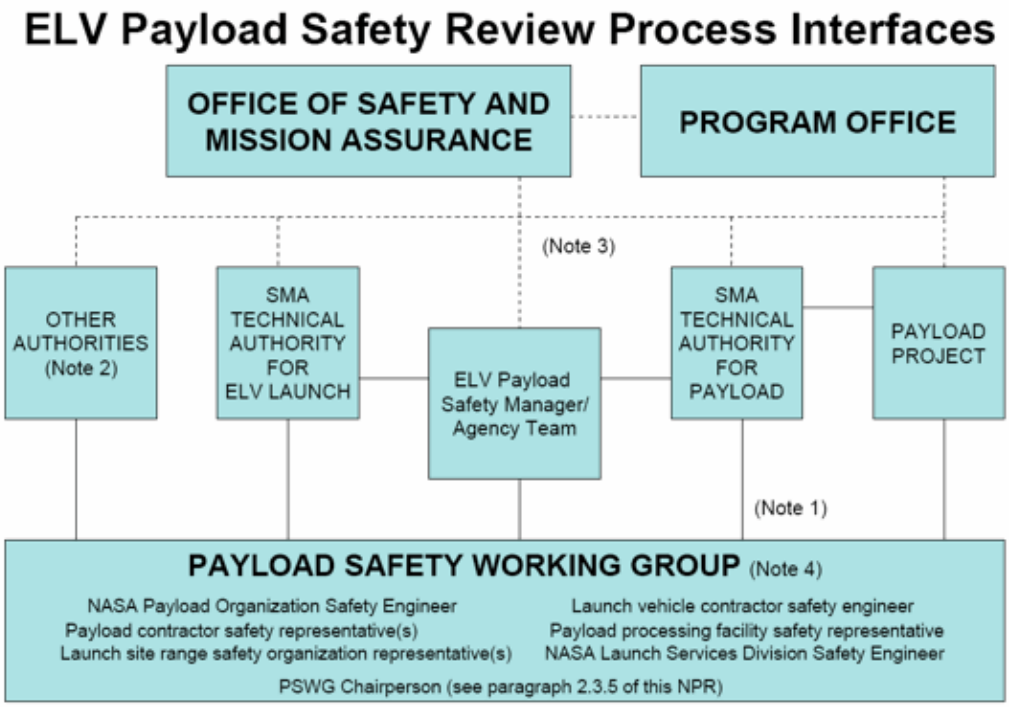
a. Assure the appropriate representation and involvement of all organizations that support the mission.

b. Identify and resolve any safety concerns as early as feasible during the project timeline.

c. Assure that the project obtains the formal approval of all required approving authorities for the mission (internal and external to the Agency).

2.2 Payload Safety Working Group

NASA ELV payload missions involve various combinations of payload organizations, payload contractors, launch vehicles, payload processing sites, and launch sites. To address this situation, a key aspect of the safety review process is the establishment of a unique PSWG for each payload. Each PSWG and its required activities are designed to ensure the appropriate involvement and coordination of all organizations that support the associated mission and share safety responsibility for the mission (internal and external to the Agency). Each PSWG ensures compliance with safety requirements that apply to its payload. Each PSWG provides clear and useful guidance to the Payload Project Office. In addition, each PSWG proactively works with the project to identify potential hazards and safety issues and advises on strategies for early abatement, mitigation, or resolution. Paragraph 2.3.1.i of this NPR identifies the organizations represented in each PSWG.



Note 1: Solid lines indicate communications that take place during a nominal safety review process. The lack of lines in this figure is not to imply that communications among the various authorities can not take place.

Note 2: Other Authorities typically include the Air Force (for launches from an Air Force Range) and may include other government agencies, international partners, or commercial payload processing facilities where applicable.

Note 3: Dashed lines indicate lines of communication that may be exercised when the safety review process identifies an issue that requires a Headquarters-level decision.

Note 4: The PSWG is the primary payload safety review interface for the project, where all initial submittals and safety concerns or issues start.

Figure 2-1, ELV Payload Safety Review Process Interfaces

2.3 Roles and Responsibilities

2.3.1 Each ELV Payload Project Manager (or designee) shall:

a. Ensure that funding and other resources are allocated for payload projects to implement a System Safety Program that complies with this NPR and NPR 8715.3 and properly implements the applicable safety requirements and successfully completes the payload safety review and approval process (Requirement 57633).

b. Ensure that the project technical development, design, test, and review processes incorporate system safety engineering in accordance with NPR 7120.5, NPR 7123.1, NPR 8715.3, and the project's System Safety Plan (see paragraph 2.5.4 of this NPR) (Requirement 57634).

c. Ensure that the design and operations of flight hardware, software, and associated GSE provide for safety through the use of approved design, analysis, and verification techniques (Requirement 57635).

d. Ensure that the payload project's timeline provides for compliance with the established payload safety review and approval process (Requirement 57636).

e. Coordinate with the local SMA organization to assign a Payload Organization Safety Engineer for the project (see paragraph 2.3.2 of this NPR) (Requirement 57637).

f. Ensure the Payload Safety Introduction Briefing (see paragraph 2.4.2.a of this NPR) is coordinated and scheduled early in Phase B as defined in NPR 7120.5 (Requirement 57638).

g. Notify the NASA ELV Payload Safety Manager of the new project and provide contact information for the appointed Payload Organization Safety Engineer (Requirement 57639).

h. Coordinate with the NASA ELV Payload Safety Manager to establish the project's PSWG and ensure that it functions as required by this NPR (Requirement 57640).

i. Coordinate with the NASA ELV Payload Safety Manager to ensure that the PSWG includes the following members, as applicable, to each mission (Requirement 57641):

(1) NASA Payload Organization Safety Engineer

(2) Payload contractor safety representative(s)

(3) Launch site range safety organization representative(s)

(4) Launch vehicle contractor safety engineer

(5) Payload processing facility safety representative

(6) NASA Launch Services Division Safety Engineer

(7) PSWG Chairperson (see paragraph 2.3.4 of this NPR)

Note: Typically, the NASA Launch Services Division Safety Engineer also serves as the PSWG Chairperson. Depending on the mission specifics, there may be advantages to having a PSWG representative from one of the other NASA organizations involved in the mission perform this function. A Co-Chairperson may also be appointed if deemed necessary for any mission.

Composition of the PSWG and member participation may vary based on project activities, technical issues, multi-Center project involvement, or operational requirements.

j. Ensure all project personnel involved in the ELV payload safety review process receive training on the process, understand their associated roles and responsibilities, and have experience commensurate with the complexity of the project (Requirement 57651).

k. Establish and implement any project-level processes and requirements needed to satisfy safety requirements and to ensure that the project fully participates in, and supports, the safety review and approval process activities identified in paragraph 2.4 of this NPR (Requirement 57652).

l. Ensure that all requirements contained in the project's tailored requirements document developed per paragraph 1.4 of this NPR are implemented for its payload and associated GSE or that the project obtains an approved waiver per paragraph 1.5 of this NPR for any requirement not satisfied (Requirement 57653).

m. Ensure spacecraft contractor oversight is defined in the Project Safety and Mission Assurance Plan required by NPR 7120.5 and performed and documented to enable safe integration, testing, and other processing of the payload and prevent the transfer of unanticipated hazards (Requirement 57654).

n. For a project existing as of the effective date of this NPR, coordinate with the PSWG and Agency Team to determine the applicability of this NPR to the remaining phases of the project (Requirement 57655).

Note: The level of implementation of the safety process defined by this NPR for projects in progress will vary with the consideration of the project's success in complying with applicable technical safety requirements, the level of inherent safety risk associated with the project, and the extent of successful completion of project safety milestones. Existing safety-related approvals and decisions will be reassessed as a result of design changes, if new mandatory safety requirements are released, or if a previously unforeseen or newly discovered safety issue is identified.

o. Ensure safety information (including safety review status and any safety concerns associated with each subsystem and integrated system) is presented at appropriate project reviews, including (but not limited to) System Requirement Reviews, Preliminary Design Reviews (PDR), Critical Design Reviews (CDR), Pre-Environmental Reviews, and Pre-Ship Reviews (Requirement 57657).

Note: The Payload Organization Safety Engineer typically presents the safety information at the various project reviews (see paragraph 2.3.2).

p. Approve all safety review and approval process deliverables per paragraphs 2.4 and 2.5 of this NPR prior to submittal to the PSWG (Requirement 57659).

q. Obtain all safety approvals and ensure safety review activities are completed in accordance with this NPR as needed to accomplish project management requirements per NPR 7120.5 and accomplish mission processing (Requirement 57660).

Note: These activities include completion of:

(1) Safety Review I in time to provide safety status and input to the project's Key Decision Point (KDP) C per paragraph 2.4.2b of this NPR .

(2) Safety Review II in time to provide safety status and input to the project's KDP D per paragraph 2.4.2c of this NPR.

(3) Safety Review III in time to provide safety approval during the project's Pre-ship Review per paragraph 2.4.2.e of this NPR.

r. Ensure that the project fully implements all safety plans and procedures required by this NPR and as approved by the PSWG (Requirement 57665).

s. Ensure that the payload design process incorporates system safety engineering activities integral to identifying hazards, developing solutions to mitigate or eliminate the hazards, verifying the implementation of these solutions, and ensuring compliance with this NPR (Requirement 57666).

t. Ensure that the status of any open items in the Safety Verification Tracking Log, the Safety Action Tracking Log, and any payload safety issues that could impact major project milestones are briefed during safety and project reviews (Requirement 57667).

u. Ensure that the PSWG Chairperson is notified of any mishaps or close calls that take place during launch area payload processing and ground operations (Requirement 57668).

2.3.2 The Payload Organization Safety Engineer for a payload project shall:

a. Perform as the payload organization's primary member of the PSWG (Requirement 57670).

b. Ensure the preparation and submittal of all safety review and approval process deliverables in accordance with schedule timeline requirements specified in paragraph 2.4 of this NPR and following the format and content requirements specified in paragraph 2.5 of this NPR (Requirement 57671).

c. Keep the Payload Project Manager informed of mission safety status (Requirement 57672).

d. Ensure that a Safety Verification Tracking Log is established, maintained, and made available for viewing electronically by the project, PSWG, and Agency Team to track closure of each open hazard control verification identified in the hazard reports (Requirement 57673).

Note: The Safety Verification Tracking Log is a deliverable for Safety Review III per paragraph 2.4.2.e.(2).(ii) of this NPR.

e. Ensure that a Safety Action Tracking Log is established and maintained for the project to track closure of safety actions (Requirement 57675).

Note: The Safety Action Tracking Log is a deliverable for Safety Reviews II and III per paragraphs 2.4.2c.(3)(iii) and 2.4.2.e.(2)(iii) of this NPR.

f. Ensure that technical operating procedures are submitted for review and approval by safety and other responsible organizations in accordance with the safety requirements of the specific operating location (Requirement 57677).

g. In coordination with the PSWG Chairperson, establish and maintain an integrated schedule of PWSG activities and all relevant project, launch, and other mission milestones, reviews, or meetings that address the topic of payload safety to include place, time, and date for each activity (Requirement 57678).

2.3.3 Each PSWG member shall:

a. Participate in the safety review and approval process (Requirement 57680).

b. Ensure compliance with all safety requirements for their area of responsibility and authority (Requirement 57681).

c. Review and provide comments to the project on all payload safety review deliverables and meeting minutes within 30 days after submittal per paragraph 2.4 of this NPR (Requirement 57682).

d. Assess and concur (or obtain concurrence from their management as needed) on tailoring and any waiver to a safety requirement that is within their scope of responsibility per paragraphs 1.4 and 1.5 of this NPR (Requirement 57683).

e. Coordinate with the PSWG to resolve payload safety concerns and, if needed, with the Agency Team (Requirement 57684).

f. Ensure that payload, facility, and payload/launch vehicle integration issues are disseminated to their organization and to other PSWG members (Requirement 57685).

g. Participate in all PSWG activities associated with their areas of responsibility, including but not limited to meetings, mission safety reviews, design reviews, ground operations reviews, and others activities as required by the PSWG Chairperson (Requirement 57686).

h. Assess and concur on plans and hazard reports for operations in facilities that fall under their safety responsibility as needed to receive and process the payload (Requirement 57687).

2.3.4 The PSWG Chairperson for a payload project shall:

a. Schedule and conduct PSWG meetings (Requirement 57689).

b. Ensure that PSWG activities and decisions include the collective input and participation from all PSWG members (Requirement 57690).

c. Provide official PSWG signature (indicating concurrence from all PSWG members) for all safety review deliverables including hazard reports, Certificate of ELV Payload Safety Compliance (see Appendix C), and any PSWG correspondence (Requirement 57691).

d. Ensure all required safety review deliverables are made available to the PSWG members and others as needed (Requirement 57692).

e. Ensure that the PSWG, the Agency Team, and the Launch Services Program representative are invited to all PSWG activities and have access to all deliverables in accordance with applicable export control requirements (see paragraph 2.6.5 of this NPR) (Requirement 57693).

f. Ensure all comments to safety review submittals are consolidated, coordinated, and furnished to the Payload Organization Safety Engineer no later than 35 days after data submittal (Requirement 57694).

g. Ensure PSWG activities are documented to include notices, scheduling, data receipt and distribution, minutes, data/document review comments, action items, key issues, decisions, and overall project status regarding completion of the safety review and approval process (Requirement 57695).

h. Ensure documentation of actions and major decisions from each PSWG meeting are reviewed for concurrence by attendees at the end of the meeting and draft minutes are available for review following the meeting (Requirement 57696).

i. Ensure distribution of final minutes within seven business days after each PSWG meeting (Requirement 57697).

j. Ensure availability/distribution/timely notification of the project safety schedule and changes to all parties involved in the safety review and approval process (Requirement 57698).

k. Ensure PSWG participation by appropriate PSWG members, as required, at payload/launch vehicle integration working group meetings (e.g., Ground Operations Working Groups, Mission Integration Working Groups) (Requirement 57699).

l. In coordination with all PSWG members, schedule and conduct PSWG meetings concurrently with major project reviews (e.g., system-level PDR and CDR) and as required to meet the safety milestones in this NPR (Requirement 57700).

Note: Throughout this NPR, "PDR" and "CDR" refer to the project's system-level PDR and CDR.

m. Ensure the Agency Team is informed of any important safety issues to include potential risk issues that may impede the safety review process, waiver issues, and safety requirements interpretation issues (Requirement 57702).

n. Ensure that all mission support and safety-related documents are made available to the PSWG members, Agency Team, the NASA ELV Payload Safety Manager, or other subject matter experts or technical authorities (Requirement 57703).

Note: The preferred approach is to use a secure Web site for this purpose.

o. If the PSWG cannot reach concurrence on an issue, the PSWG Chairperson shall coordinate with the NASA ELV Payload Safety Manager to establish a resolution approach (Requirement 57705).

p. Coordinate with the PSWG and the project to ensure implementation of recommendations, interpretations, and resolutions of any safety concern provided by the Agency Team (Requirement 57706).

Note: The PSWG Chairperson also has responsibilities under the Tailoring Process per paragraphs 1.4.3 and 1.4.4 of this NPR.

2.3.5 The NASA Launch Services Program Manager (or designee), for payloads launched via the Launch Services Program, shall:

a. Provide the funding and other resources needed to ensure that personnel from the launch vehicle contractor (once under contract), Launch Services SMA, and the Range participate in the safety review process beginning no later than the Payload Safety Introduction Briefing (see paragraph 2.4.2 a. of this NPR) and to acquire payload processing facilities (Requirement 57709).

b. Provide the funding and other resources needed to ensure the acquisition and preparation of payload processing facilities for use by the Payload Organization (Requirement 57710).

c. Notify the PSWG of program integration meetings including Ground Operations Working Group, Ground Operations Review, Mission Integration Working Group, and others (Requirement 57711).

d. Ensure that the NASA Launch Services Division Safety Representative is notified of any payload/launch vehicle interface safety concerns (Requirement 57712).

e. Ensure launch services contracts for launch vehicle and commercial payload processing facility contracts contain the provisions needed to satisfy the requirements of this NPR (including requirements incorporated by reference) (Requirement 57713).

2.3.6 The NASA ELV Payload Safety Manager (or designee) shall:

a. Track the status of each payload project as it proceeds through the safety review and approval process and provide guidance on the associated activities, tools, and deliverables as needed (Requirement 57715).

b. Notify the Payload Project Manager and other authorities:

(1) If a major safety-related risk that may adversely impact the project is identified any time during this safety review process (Requirement 57717).

(2) If the required safety review activities or deliverables of this NPR are not met (or product quality is inadequate for that phase of the project lifecycle) and fail to fulfill the required safety gate products prior to the project's KDPs per NPR 7120.5 and provide guidance on how the project should proceed (Requirement 57718).

c. Sign the Certificate of ELV Payload Safety Compliance upon ensuring that all Agency Team concerns have been addressed (Requirement 57719).

d. Issue a letter forwarding the Certificate of ELV Payload Safety Compliance to the Payload Project Manager and others signifying the successful completion of the ELV Payload Safety Review III and readiness to proceed with shipping and processing (see paragraphs 2.4.2.e and 2.4.3 of this NPR) (Requirement 57720).

Note: The NASA ELV Payload Safety Manager's overall responsibilities for the ELV Payload Safety Program are provided in paragraph 1.3.3 of this NPR.

2.4 Flow of Activities and Deliverables

2.4.1 In accordance with the roles and responsibilities specified in paragraph 2.3 of this NPR, the Payload Project Manager or designee and the PSWG Chairperson are responsible for ensuring that the payload safety review and approval activities take place as required in paragraph 2.4.2 of this NPR. The Payload Organization Safety Engineer ensures the preparation and submittal of the associated deliverables for review. Requirements regarding the contents of the deliverables are specified in paragraph 2.5 of this NPR.

Note: The safety review and approval activities are designed to coincide with and provide safety input to the project management reviews required by NPR 7120.5; e.g., PDR, CDR, and Pre-ship Review. The safety review and approval activities identified below may also provide safety input to other required project, Center, and NASA Headquarters reviews; e.g., Peer Reviews, Launch Readiness Reviews, and Safety and Mission Success Reviews.

2.4.2 The payload project and the PSWG shall ensure that the safety review and approval process incorporates the following sequence of activities and associated deliverables, including compliance with the associated required schedule timing of deliverables (Requirement 57725).

Exception: Process and deliverable dates required by this NPR may be altered through advanced formal agreement between the Payload Project Office and the PSWG provided that safe processing, project schedule, and safety review input to KDPs as defined in NPR 7120.5 are not impacted.

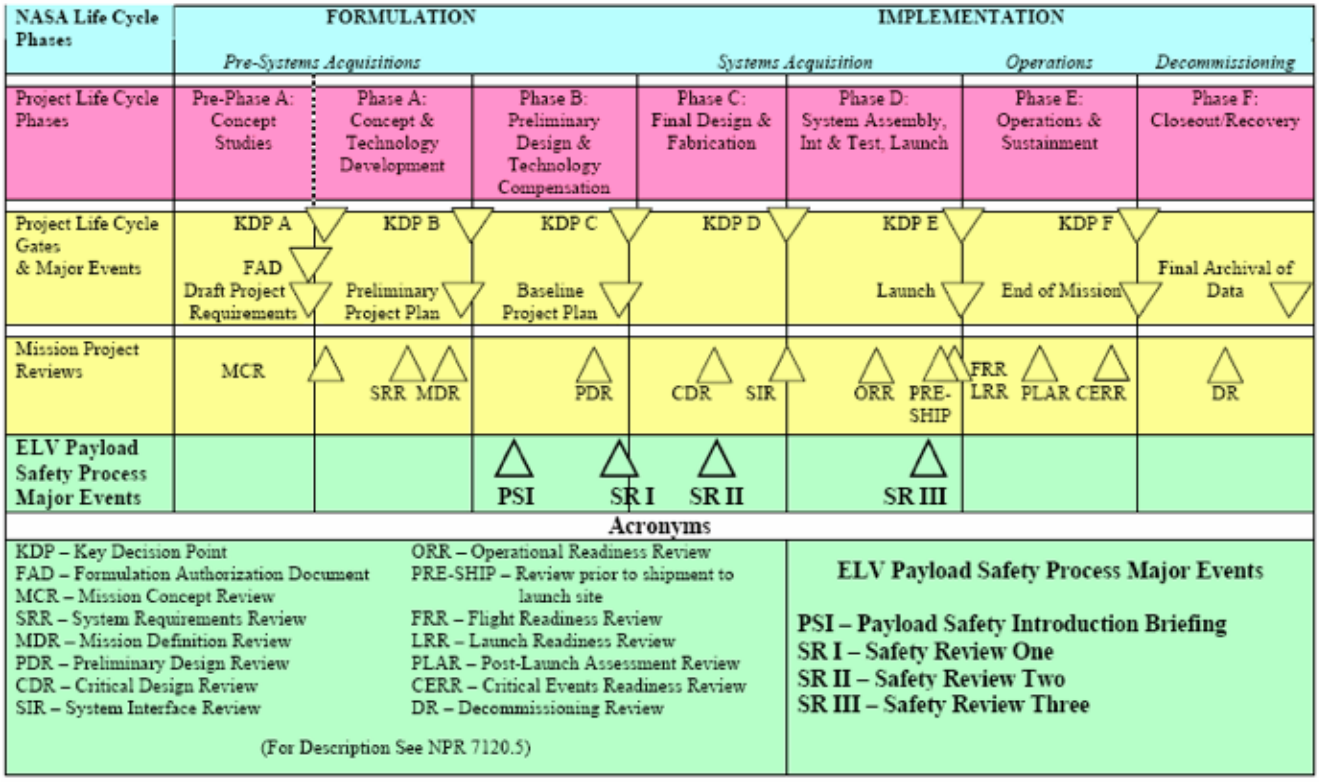


Figure 2-2, Timeline of ELV Payload Safety Program Reviews

Note: The ELV Payload Safety Reviews shown in Figure 2-2 are conducted by a project's PSWG in order to provide necessary safety status and input to the Mission Project Reviews and the project's KDPs.

a. A Payload Safety Introduction Briefing (See definition in Appendix A) shall occur as early as possible but no later than midpoint of the Preliminary Design Phase (Phase B as defined in NPR 7120.5 and depicted in Figure 2-2) (Requirement 57728). This is typically the first meeting of the PSWG. The payload project shall submit:

(1) As a precursor to the tailoring processes, identification of the safety requirement documents that are applicable to the project; applicable previously approved waivers and alternative approaches; and known tailoring issues for presentation and review during the Payload Safety Introduction Briefing (Requirement 57729).

(2) Draft Systems Safety Plan that, as a minimum, provides a conceptual overview of the Systems Safety Program for presentation and review at the Payload Safety Introduction Briefing (Requirement 57730).

(3) Identification of known spacecraft/payload systems and a preliminary assessment of potential hazards documented in a preliminary hazard list for presentation at the Payload Safety Introduction Briefing (Requirement 57731).

(4) A basic Ground Operations Flow Overview providing the location and timeline of major payload activities and tasks for presentation at the Payload Safety Introduction Briefing (Requirement 57732).

Note: This briefing provides a forum for the project to introduce the mission to the PSWG and other authorities and allows for early identification of any safety concerns associated with the payload. The information provided at this briefing should be as complete as the technical maturity of the conceptual design and operations allow.

b. Safety Review I begins with the submittal of data prior to the PDR per paragraph 2.4.2.b.(3) and shall be completed no later than 60 days after the project's PDR or no later than necessary to provide the PSWG's input to the project's KDP C as defined in NPR 7120.5 and depicted in Figure 2-2, whichever date comes first (Requirement 57734).

(1) Safety Review I shall include a PSWG meeting held in conjunction with the PDR (Requirement 57735).

(2) During Safety Review I, the PSWG shall approve the final System Safety Plan, discuss the resolution of comments to the Safety Data Package (See Appendix A for definition), address requirements issues through the review of the tailored requirements, assess the Preliminary Hazard Analysis and any Hazard Reports, and address any safety issues identified during the PDR (Requirement 57736).

(3) The Payload Project shall submit the following material prior to the PDR meeting:

(i) Final System Safety Plan no later than 30 days prior to the PDR meeting (Requirement 57738).

(ii) Tailored Payload Safety Requirements no later than 30 days prior to the PDR meeting (Requirement 57739).

(iii) Safety Data Package I (as complete as possible) no later than 30 days prior to the PDR Review (Requirement 57740).

(4) The PSWG Chairperson shall provide the Payload Project Manager with the status of Safety Review I including any safety concerns following the PDR meeting (Requirement 57741).

(5) Safety Review I shall culminate with the PSWG Chairperson providing the Payload Project Manager with an assessment of the project's safety efforts and identification of any safety concerns to support the project's KDP C (as defined in NPR 7120.5) (Requirement 57742).

c. Safety Review II begins with the submittal of data prior to the project's CDR per paragraph 2.4.2.c.(3) and shall be completed no later than 60 days after the project's CDR to provide the PSWG's input to the project's KDP D as defined in NPR 7120.5 and depicted in Figure 2-2 (Requirement 57743).

(1) Safety Review II shall include a PSWG meeting held in conjunction with the CDR (Requirement 57744).

(2) During the Safety Review II, the PSWG shall discuss the resolution of comments to the Safety Data Package I, discuss any safety issues identified during the CDR, and review the project for any changes to the design, processing, or interfaces for new or increased hazards or safety issues (Requirement 57745).

(3) The payload project shall submit:

(i) Safety Data Package II no later than 30 days prior to the Safety Review II meeting (Requirement 57747).

(ii) Final Tailored Payload Safety Requirements no later than 30 days prior to the Safety Review II meeting (Requirement 57748).

(iii) The project Safety Action Tracking Log for concurrence to close completed actions and to review open actions and status (Requirement 57749).

(4) Safety Review II shall culminate with the PSWG Chairperson providing the Payload Project Manager with an updated assessment of the project's safety efforts and identification of any safety concerns to support the project's KDP D (as defined in NPR 7120.5) (Requirement 57750).

d. If the payload will undergo processing at a NASA-owned facility or any facility where NASA personnel control the operation or are actively involved in performing work prior to the Safety Review III (see paragraph 2.4.2.e of this NPR), the project shall coordinate to define the applicable requirements and processes for safe payload processing at the host Center that meet the intent of the requirements defined in this NPR (Requirement 57751).

e. Safety Review III begins with the submittal of data per this paragraph 2.4.2.e(2) of this NPR and shall be completed at a PSWG meeting held at least five business days prior to the Launch Services Program's Ground Operations Review which is held before the Payload Project's Pre-ship Review (see Figure 2-2) (Requirement 57752).

Note: Scheduling of the Safety Review III PSWG meeting is done in coordination with the Launch Services Program and the Payload Project. Typically, the Launch Services Program schedules the Ground Operations Review 30 days prior to scheduled hardware arrival at the launch area, and it is held prior to the Payload Project's Pre-ship Review. Completion of Safety Review III allows the PSWG to be prepared to support the Ground Operations Review and present the project's safety status and any issues.

(1) During Safety Review III, the PSWG shall verify that all safety requirements have been satisfied or will be satisfied at the appropriate time or any associated waivers have been approved (Requirement 57754).

(2) The payload project shall submit:

(i) A Safety Data Package III no later than 60 days prior to the Safety Review III, and it shall be finalized satisfying all comments at least 30 days before the intended shipment of hardware to the prelaunch payload processing site (Requirement 57756).

(ii) A Safety Verification Tracking Log identifying the open verifications from the Hazard Reports (Requirement 57757).

(iii) A Safety Action Tracking Log current to the Safety Review III meeting for concurrence to close completed actions and to review open actions and status (Requirement 57758).

(3) The project shall provide a Certificate of ELV Payload Safety Compliance, signed by the Project Manager, with signature blocks for the PSWG Chairperson and the ELV Payload Safety Manager (Requirement 57759).

(4) Safety Review III shall culminate with the PSWG Chairperson and the ELV Payload Safety Manager signing the Certificate of ELV Payload Safety Compliance indicating that the project has safety approval to ship the payload to

the launch area (Requirement 57760).

2.4.3 The ELV Payload Safety Manager shall provide the Payload Project Manager with a letter (or equivalent) within 5 days of successful completion of Safety Review III with copies to other officials as appropriate for each mission (Requirement 57761). The letter shall:

a. Indicate that the project has successfully completed the payload safety review process per this NPR (Requirement 57762).

b. Include a copy of the signed Certificate of ELV Payload Safety Compliance including any addendum (Requirement 57763).

c. Identify all conditions or constraints applicable to the safety approvals (Requirement 57764).

2.4.4 After transportation of the payload to the launch area processing facility, the project shall update the Safety Verification Tracking Log at least weekly (more frequently if the open items must be closed to remove operational constraints) and make the current Safety Verification Tracking Log available to all officials involved in the mission (Requirement 57765).

2.5 Content of Deliverables

2.5.1 The Payload Organization Safety Engineer, in coordination with other payload project personnel as needed and the PSWG, shall:

a. Ensure that the content of the safety review process deliverables satisfies the requirements of paragraph 2.5.2 through 2.5.10 of this NPR (Requirement 57768).

b. Ensure that the level of technical detail for each safety review process deliverable is commensurate with the project's life-cycle phase (Requirement 57769).

c. Ensure that changes to deliverables are annotated in such a way that each change is easily located and verified by the reviewer (Requirement 57770).

2.5.2 Tailored Payload Safety Requirements shall:

a. Document all safety requirements that apply to a payload mission (Requirement 57772).

b. Use Air Force Space Command Manual (AFSPCMAN) 91-710, Range Safety User Requirements Manual as the baseline document for tailoring and include any applicable NASA and local safety requirements that are in addition to those in AFSPCMAN 91-710 (Requirement 57773).

c. In the event of conflicting requirements, incorporate the more stringent (Requirement 57774).

Note: A majority of safety requirements applicable to NASA ELV payloads are currently documented in the Air Force requirements document, AFSPCMAN 91-710. NASA and the USAF(30th and 45th Space Wings) have tentatively agreed to jointly develop requirements for ELV payload safety. NASA and Air Force payload safety requirements will be merged into a mutually agreeable tailoring template, which will serve as the baseline for all ELV payload safety tailoring.

d. Document the applicability of safety requirements to specific situations within a mission (Requirement 57776).

e. Document the interpretation of requirements as needed (Requirement 57777).

f. Address any recommendations, interpretations, or resolutions of safety concerns provided by the Agency Team and each authority involved in the mission (Requirement 57778).

g. Identify any change to a requirement (i.e., any addition or deletion from the source requirement) and include sufficient rationale for the tailored change (Requirement 57779).

h. Identify potential areas of noncompliance with applicable requirements (Requirement 57780).

i. Reference any waivers identified during the tailoring process (see paragraphs 1.4.8 and 1.5 of this NPR) (Requirement 57781).

2.5.3 A Payload Safety Introduction Briefing shall provide the following information to a level of detail consistent with the complexity of the mission, the maturity of the conceptual design, and determination of the launch vehicle and launch site location:

a. Overview of the System Safety Program as defined by the project's System Safety Plan (see paragraph 2.5.4 of this NPR) (Requirement 57783).

b. Identification of organizational roles and responsibilities (Requirement 57784).

c. Identification of applicable safety requirements and compliance documents (Requirement 57785).

d. Description of payload, instruments, and anticipated ground support equipment (Requirement 57786).

e. Description of the flight path in terms of azimuth and trajectory. Identification and description of planned recovery activities and support for sample/payload return if applicable (Requirement 57787).

f. Identification of potential payload/launch vehicle interfaces and mission-unique ground support equipment required for pad operations (Requirement 57788).

g. Identification and a preliminary assessment of potential hazards associated with payload to launch vehicle integration, multiple payloads, and ground systems documented in a preliminary hazard list (Requirement 57789).

h. Overview of Draft Requirements Tailoring, identifying critical assumptions to be made during the tailoring process (Requirement 57790).

i. Identification of any potential noncompliances to NASA, NASA Center, commercial processing facility, Air Force Range, Federal, State, or local requirements (Requirement 57791).

j. Any potential hazardous failure modes, failure probability, and performance characteristics of the payload during ground operations (Requirement 57792).

k. Identification of planned studies and analyses that support safety requirements, including scheduled completion (Requirement 57793).

l. Description of processing flow and anticipated schedule, integrated with major project milestones (Requirement 57794).

m. Identification of facility requirements, including launch complex, hazardous assembly and checkout areas, and ordnance and propellant storage requirements (Requirement 57795).

n. Identification and discussion of potential contingency operations, for example, depressurization, propellant offload, and accessibility after fairing installation (Requirement 57796).

o. Overview of the Mishap Preparedness and Contingency Plan(s) and their approach for communicating, documenting, and investigating payload prelaunch contingencies including close calls, lessons learned, and mishaps; potential project specific emergency response; and anticipated data impound responsibilities as required by NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping (Requirement 57797).

p. Recommendations for future safety Technical Interchange Meetings, reviews, working groups, subject matter expert support, resolution of unmet requirements, Design Reviews, and other topics as deemed necessary (Requirement 57798).

2.5.4 A System Safety Plan encompassing the payload project's complete system safety program consistent with NPR 8715.3, shall include:

Note: MIL-STD-882, Department of Defense Standard Practice for System Safety also provides guidance for a system safety program.

a. A system safety roles and responsibilities section describing:

(1) Interfaces and lines of communication with associated organizations including decision-making timelines and a description of the methods by which personnel may raise issues of concern to the project manager (Requirement 57802).

(2) Review and approval process (including identification of approving authorities) for commitment of assets to safety efforts (Requirement 57803).

(3) The staffing and responsibilities of key system safety personnel (Requirement 57804).

(4) The tasks and activities required to identify, evaluate, and eliminate or control hazards and to minimize risk (Requirement 57805).

b. System Safety Program Milestones identifying and scheduling safety tasks and activities such as design analyses, tests, and reviews and relating them to major project (mission) milestones (Requirement 57806).

c. System Safety Data identifying deliverable as well as non-deliverable data by title, number, date, and means of delivery or process for accessibility (Requirement 57807).

d. System Safety Interfaces identifying:

(1) The interfaces between system safety and other applicable safety disciplines such as nuclear safety, facility or institutional safety, range safety, explosive and ordnance safety, chemical and biological safety, radiation safety,

hazardous materials safety, fire safety, laser safety, software safety, and any others (Requirement 57809).

(2) The interfaces between system safety and design systems engineering (Requirement 57810).

(3) The interfaces between system safety and other support disciplines such as maintainability, quality, reliability, software development, human factors engineering, occupational health, environmental health, and any others (Requirement 57811).

(4) The interface between system safety and all system integration and test disciplines (Requirement 57812).

2.5.5 Preliminary Hazard Assessments and Hazard Reports

a. The payload project shall utilize system safety engineering and analyses to identify potential hazards associated with the payload and to determine how those hazards will be eliminated or controlled (Requirement 57814).

b. The preliminary hazard analyses presented at the time of the Payload Safety Introduction Briefing shall reflect the payload conceptual design, planned interfaces, operations, and identify potential hazards (Requirement 57815).

c. Hazard Reports shall document:

(1) Each hazard, the mechanism(s) for potential occurrence, and resulting outcome (Requirement 57817).

(2) The worst case severity and probability associated with each hazard (Requirement 57818).

(3) The planned mitigations (specific methods for controlling the safety risk associated with each hazard) (Requirement 57819).

(4) How control of the safety risk associated with each hazard will be verified (Requirement 57820).

Note: The status of these verifications is tracked during payload development and processing in a Safety Verification Tracking Log (see paragraph 2.5.9 of this NPR).

(5) The severity and probability associated with each hazard with the mitigations in place (Requirement 57822).

(6) Compliance with the safety requirements applicable to each hazard (Requirement 57823).

2.5.6 Safety Data Package I shall include:

a. Descriptions of hazardous and safety critical flight hardware and software, systems, components, and materials that comprise the payload and ground support equipment and reflect the PDR-level design and operations scenario of the payload (Requirement 57825).

b. A description of the payload and mission (Requirement 57826).

c. Initial descriptions of all payload systems including hazardous and safety critical subsystems, their operation, and interfaces (Requirement 57827).

d. Preliminary hazard reports (as defined in 2.5.5 of this NPR) and summaries of the hazard analyses performed on payload systems (Requirement 57828).

e. Information identifying compliance to the Tailored Payload Safety Requirements (Requirement 57829).

f. For a project utilizing a previously launched payload bus, identification and description of any payload safety-related problems, mishaps, or failures that occurred during fabrication, testing, processing, or integration that could affect the safety of the flight hardware or software, ground support equipment, personnel, or other NASA resources (Requirement 57830).

2.5.7 Safety Data Package II shall include:

a. Updated Safety Data Package I information that reflects the CDR-level design and operations scenario of the payload (Requirement 57832).

b. An updated description of the payload and mission scenario (Requirement 57833).

c. Updated Hazard Reports (as defined in 2.5.5 of this NPR) (Requirement 57834).

d. Detailed narrative descriptions of hazardous and safety critical subsystems, their operation, and updated information identifying methods of compliance to the Tailored Payload Safety Requirements (Requirement 57835).

e. Detailed information of safety features, inhibits, monitoring systems, and their control and status during all processing phases (integration, test, prelaunch, launch, and return (if applicable)) (Requirement 57836).

f. Supporting plans, studies, and reports (provided or referenced), and furnished upon request (Requirement 57837).

g. A description of the ground support equipment, summary of hazardous, non-hazardous, and safety critical operations, a list of hazard reports, and supporting hazard analyses for operations performed in NASA facilities,

NASA contracted facilities, and at launch site facilities (i.e., Ground Operations Plan) (Requirement 57838).

h. A cross-reference identifying the disposition of PSWG and Agency Team review comments of Safety Data Package I to indicate where incorporated changes to the Safety Data Package were made (Requirement 57839).

2.5.8 Safety Data Package III shall include:

a. All the Safety Data Package updates and address all comments and incorporate all changes that reflect the as-built configuration and planned processing activities (Requirement 57841).

b. The final as-built description of the payload and mission scenario (Requirement 57842).

c. Final Hazard Reports (as defined in 2.5.5 of this NPR) (Requirement 57843).

d. Updated narrative descriptions of hazardous and safety critical subsystems (Requirement 57844).

e. Updates to supporting plans, studies, and reports; required summaries of test results shall be provided and furnished upon request (Requirement 57845).

f. A record of test failures, anomalies, and mishaps involving qualification hardware, flight hardware, ground support equipment, and software (if used for hazard control), and an assessment of the resolution and safety implications of these events (Requirement 57846).

g. A signed copy of any approved safety waivers (with attachments provided upon request) (Requirement 57847).

h. A cross-reference identifying the disposition of review comments since the last Safety Data Package submittal to indicate where incorporated changes to the Safety Data Package were made (Requirement 57848).

2.5.9 Safety Verification Tracking Log

a. The Safety Verification Tracking Log for a payload project shall document (in a tabular format) the status of the safety verifications identified in the project's Hazard Reports (see paragraph 2.5.5 of this NPR) (Requirement 57850).

b. For each safety verification, the Safety Verification Tracking Log shall list a safety verification tracking number, a brief description of the safety verification, the applicable Hazard Report number(s), the operation(s) constrained by the safety verification, whether independent verification is needed, scheduled and actual completion dates, method of closure, status ("Open" or "Closed"), and any comments (Requirement 57851).

Note: A "Closed" entry in the Safety Verification Tracking Log indicates that mitigations are in place and that the safety risk associated with the hazard is controlled as specified in the associated Hazard Report. Safety verifications often are best performed at a certain time in the payload processing flow. The Safety Verification Tracking Log is a required submittal by the payload project for Safety Review III (see paragraph 2.4.2e.(2) and is used to ensure the completion of safety verifications even after transportation of the payload to the launch area processing site (see paragraph 2.4.4).

2.5.10 A Safety Action Tracking Log

a. The Safety Action Tracking Log for a payload project shall document (in tabular format) the status of safety-related actions generated from the safety reviews and other safety meetings (Requirement 57854).

b. For each action, the Safety Action Tracking Log shall list an action number, a brief description of the action, the responsible person(s), scheduled and actual completion dates, status ("Open" or "Closed"), and any comments (Requirement 57855).

Note: The Safety Action Tracking Log is a required submittal by the payload project for Safety Review II and Safety Review III (see paragraphs 2.4.2c.(3) and 2.4.2e.(2)) and may also be used by the PSWG Chairperson to record and track actions (see paragraph 2.3.4g).

2.6 Data Submittals

2.6.1 Each payload project shall make data submittals electronically using a NASA secure electronic knowledge management system approved by the PSWG and the ELV Payload Safety Manager (Requirement 57858).

2.6.2 The Payload Project Office shall manage the submission of data to ensure NASA information technology requirements are met; where applicable, ensure access by the PSWG, Agency Team, and others as designated; and that submittals are legible and uploaded in English (Requirement 57859).

2.6.3 All parties shall ensure that NPR 2810.1, Security of Information Technology is followed and that safety data from one project is not shared with unauthorized persons including persons participating on a different project (Requirement 57860).

2.6.4 If a payload project deems it necessary to submit deliverables by an alternative method, the project shall obtain approval from the PSWG and the ELV Payload Safety Manager (Requirement 57861).

Note: A payload project may submit deliverables via electronic mass storage media devices to the PSWG Chairperson who will ensure the deliverables are placed on a secure Web site.

2.6.5 Export Controlled Data

a. The export control data submittal requirements shall apply to U.S. Payload Project Offices only in accordance with NPR 2190.1, NASA Export Control Program (Requirement 57864).

b. Foreign Payload Project Offices are not normally required to provide the U.S. export control classification of their deliverables.

c. In the event that a foreign deliverable requires a U.S. export control classification, NASA export control resources shall be used to classify it (Requirement 57866).

2.6.6 Proprietary Data and Sensitive But Unclassified (SBU)

a. The Payload Project Office and source of data shall determine the necessary requirements for SBU and proprietary data (Requirement 57868).

b. The Payload Project Office shall implement the requirements and provide appropriate instruction (Requirement 57869).

c. The Payload Project Office shall ensure that SBU and proprietary data are distributed only to persons who have a need to review such data in support of the safety review process (Requirement 57870).

Note: Typically the PSWG, NASA ELV Payload Safety Manager, Agency Team, and all other participating parties, as deemed necessary by the PSWG Chairperson or NASA ELV Payload Safety Manager, will have access to the secure project safety data. It is the responsibility of all parties to follow NASA requirements for controlling the data.

d. If the Payload Project Office discovers that the classification of data has changed, the Payload Project Office shall inform the PSWG and Agency Team in writing (Requirement 57872).

| TOC | Preface | Chapter1 | Chapter2 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS